LAB MANUAL
ON
BUG & BOUNTY

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION

SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Purnima Mohanty (Project Assistant)

Table of Contents

Introduction to Bug & Bounty

Security Bug

A security bug or security defect is a software bug that can be exploited to gain unauthorized access or privileges on a computer system. Security bugs introduce security vulnerabilities by compromising one or more of Authentication of users and other entities. Security bugs introduce security vulnerabilities by compromising one or more of:

- Authentication of users and other entities
- Authorization of access rights and privileges
- Data confidentiality
- Data integrity

On September 9, 1947, a team of computer scientists and engineers reported the world's first computer bug. A bug is a flaw or glitch in a system. Thomas Edison reported "bugs" in his designs as early as the 1800s, but this was the first bug identified in a computer. First case of bug being found," one of the team members wrote in the logbook. The team at Harvard University in Cambridge, Massachusetts, found that their computer, the Mark II, was delivering consistent errors. The first report of bug was delivered by Grace Hopper.

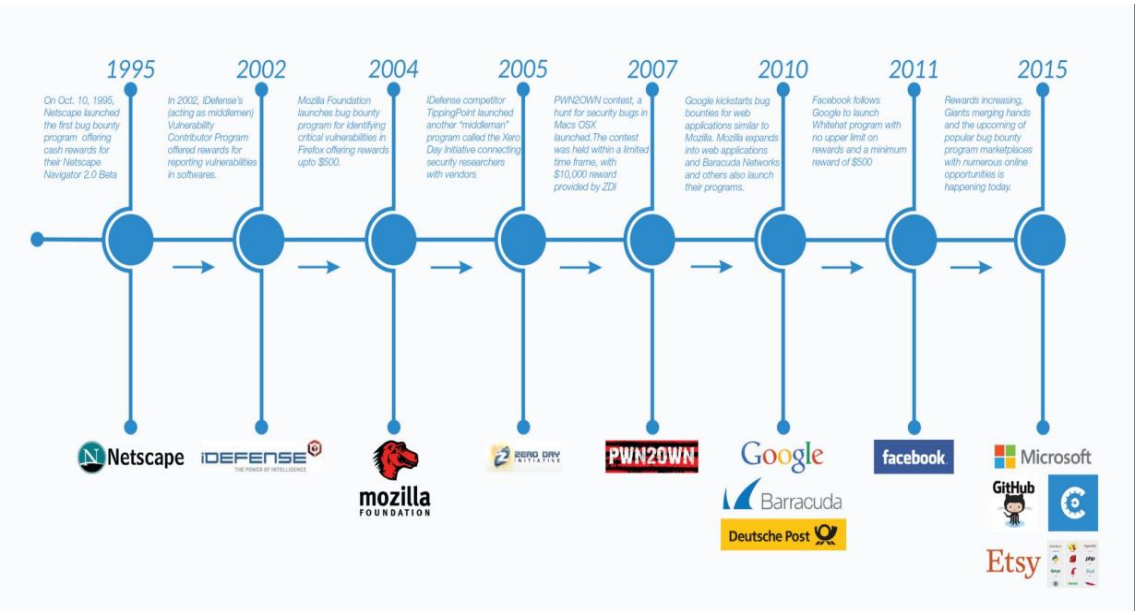
What is Bug Bounty?

A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Bug bounty programs have been implemented by a large number of organizations. A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

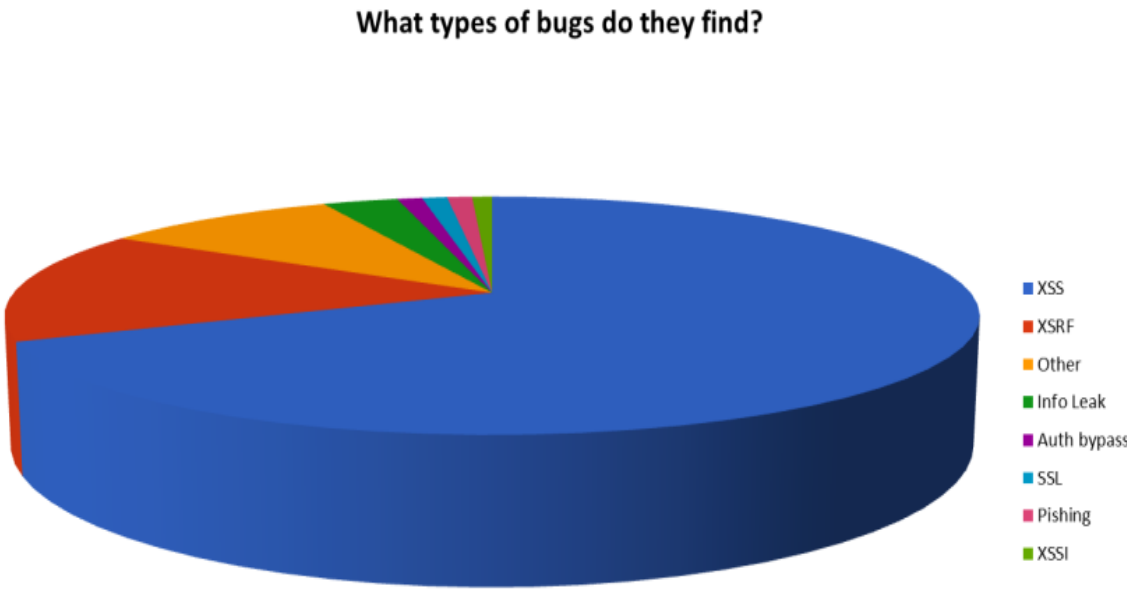
History of Bug Bounty

Three years back when Ola was hacked, compromising the data of millions of users, they created India’s first full-fledged bug bounty program to encourage independent security researchers to help them create a safe platform. The company now offers up to 3,00,000 INR for security loopholes such as injections, server-side issues, client-side issues, and other valid security vulnerabilities. Ola has seen success with its program. Security research bloggers from Fallible say Ola awarded them with $1000 in bounty and some electronic goodies for reporting vulnerabilities in one of their apps. The researchers also

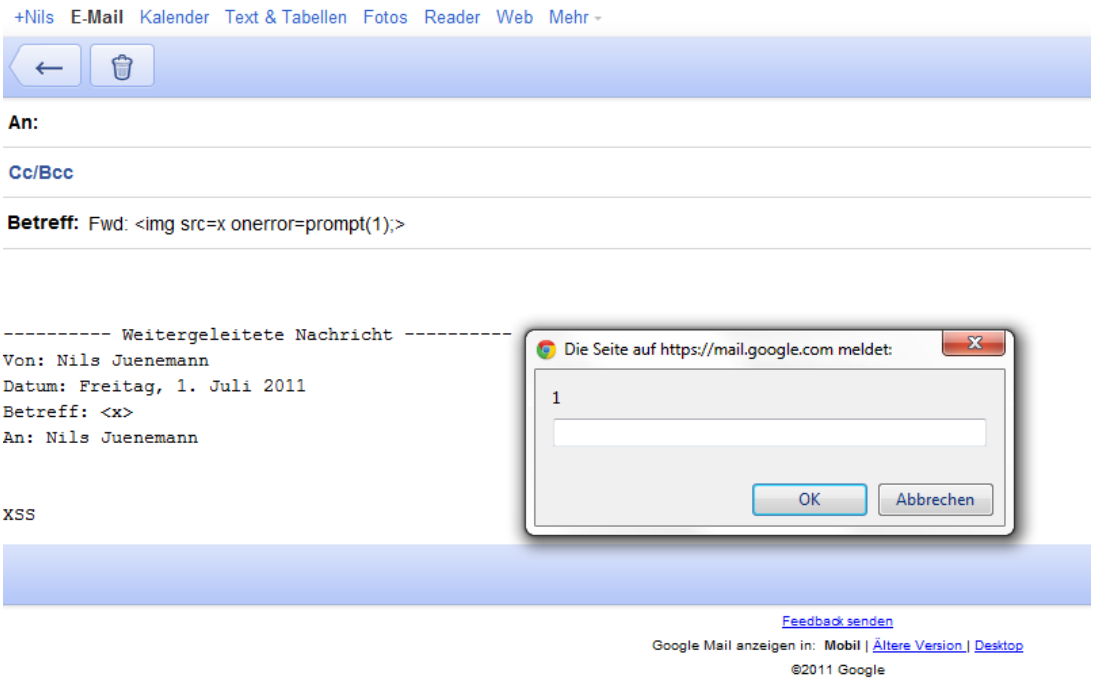
claim Ola took around 2 months to fix their reported bug. McDonalds India (West and South) runs a bug bounty program in India for its web and mobile apps for McDelivery. In 2017, researchers from Fallible discovered a huge vulnerability in their app. They found it was possible for hackers to dump the data of 2.2 million users by exploiting a flaw. Paytm is another company running a bug bounty program in India. Avinash Jain, an independent security researcher found a vulnerability in Paytm's electricity bill payment service. Sandeep reveals bug bounty hunting allows you to be your own boss, and work with freedom and flexibility.From 2016, nullcon has started a BountyCraft Track. It is a platform where the Bug Bounty Program offering companies (Microsoft,Apple, Google) & crowdsourced security platforms (Bugcrowd, Hackerone, NCC Group, Crowdfense) interact directly with Bug



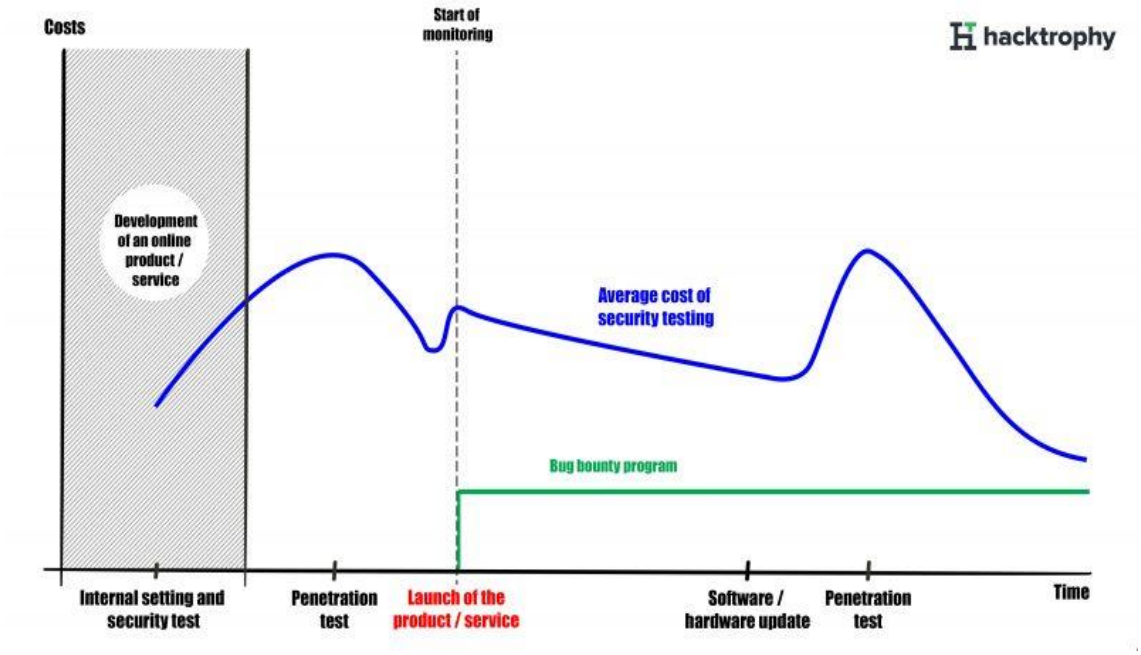
Graphical Report



Sample of Bug Bounty XSS found in Mail

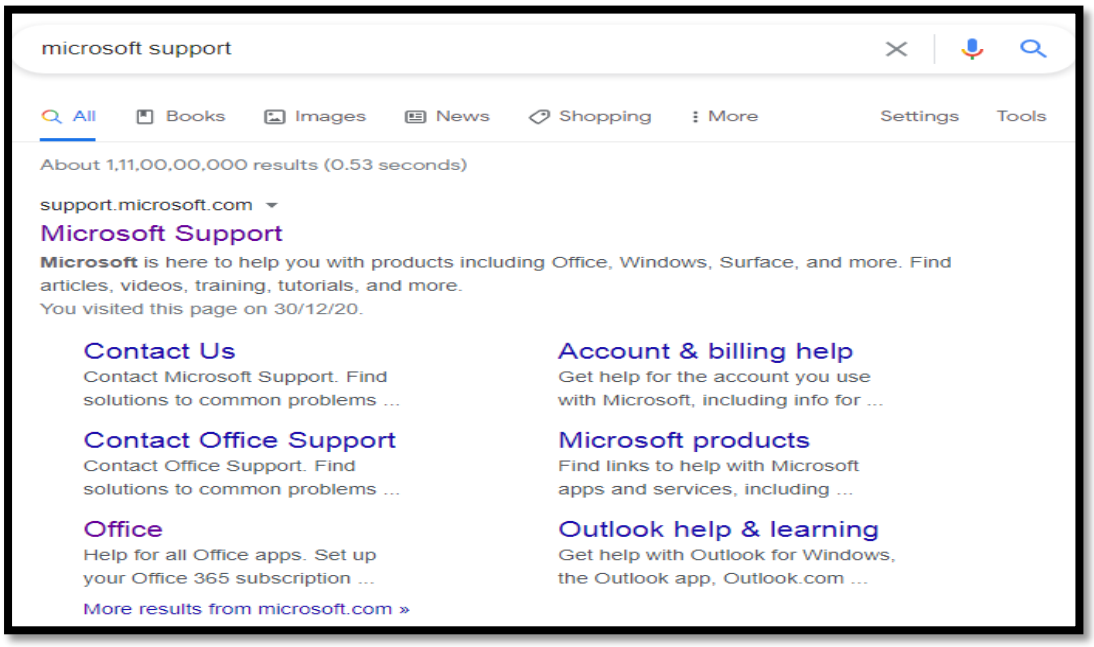


The objective is to search for organizations that announce and provide a professional and transparent ecosystem for carrying out security testing, reporting and payments, while indemnifying the tester from any legal or other action. Permission will be obtained from the organization that has announced the program. At the very least, a record of start date, end date and access times will be maintained and may be shared with the organization if needed. Vulnerability will be exploited only for the purpose of getting a screenshot of the extent of penetration into the organization's infrastructure. All testing will be non-destructive. Making changes in source code of programs running on the organization infrastructure or in documents stored on the systems to which access has been obtained. No data or documents will be copied from any of the vulnerable systems on which access has been obtained during the course of searching for bugs and vulnerabilities. No testing will be done for "information" or "knowledge enhancement" purposes as this is a professional activity and one expects to earn from the same. Payments as per the payout norms of the organizing company will be accepted without dispute. Any bug / vulnerability / issue that is reported under a bug bounty program will be released in public only after it has been repaired by the affected organization.

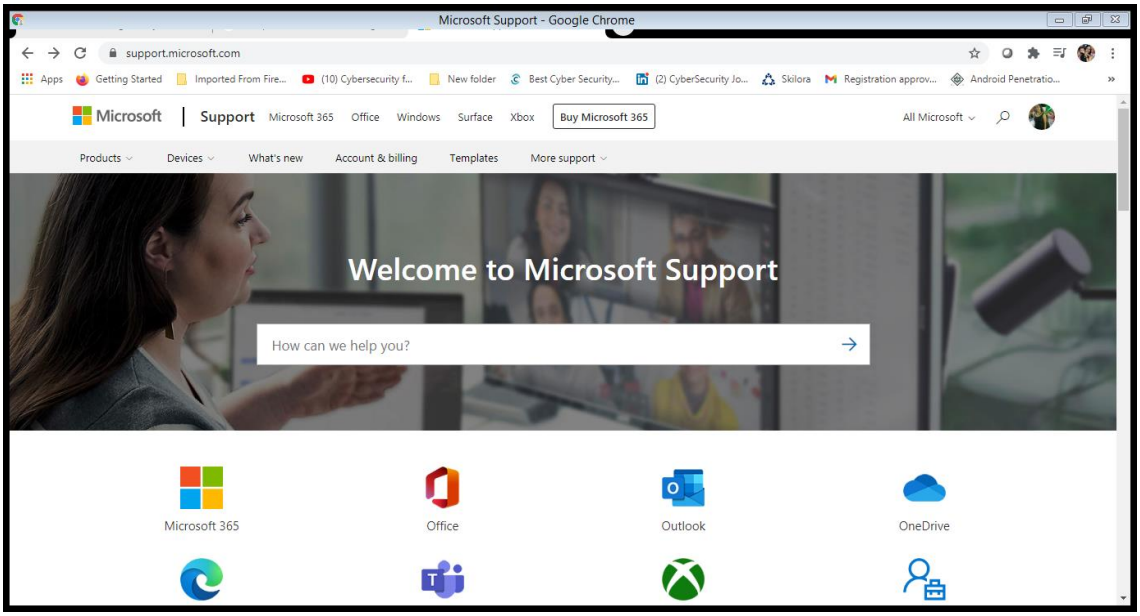

Costs
Start of monitoring
hacktrophy
Development of an online product / service
Average cost of security testing
Bug bounty program
Internal setting and security test
Penetration test
Launch of the product / service
Software / hardware update
Penetration test
Time

Installation of Visual Studio

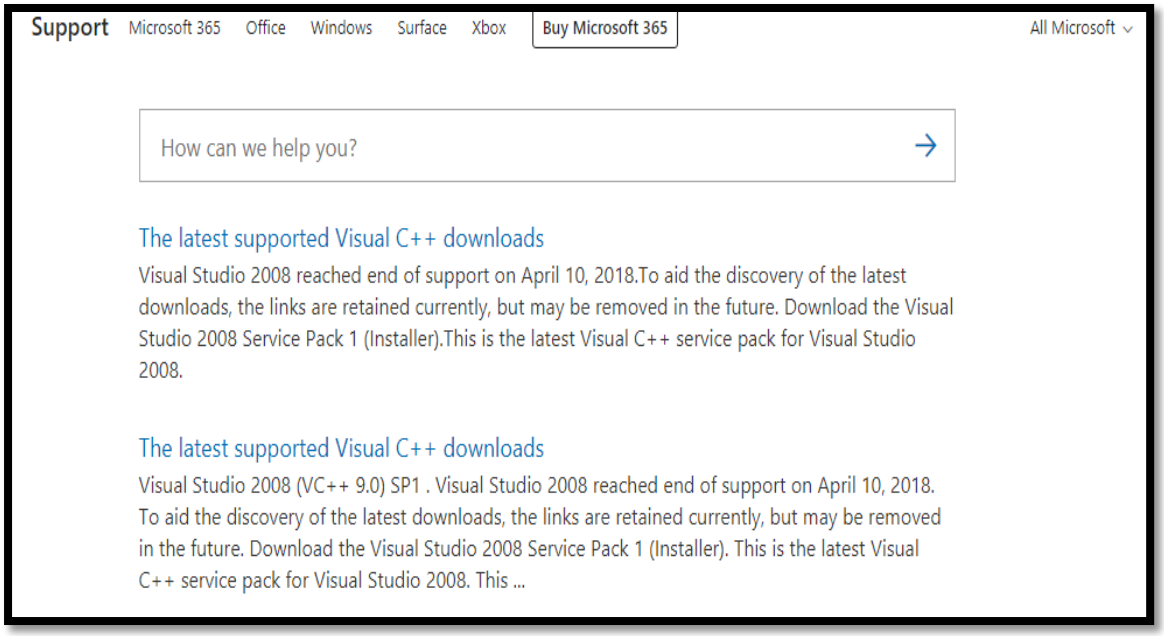
Step 1:- Open google website and type “Microsoft support”



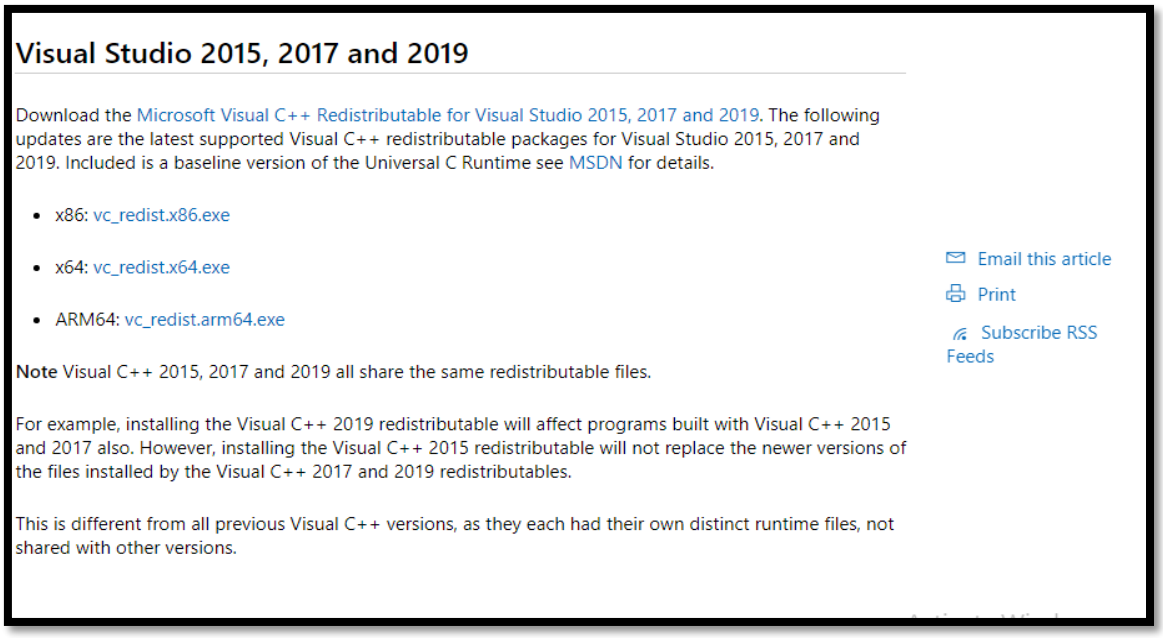
Step 2:- After getting the page type visual studio in search



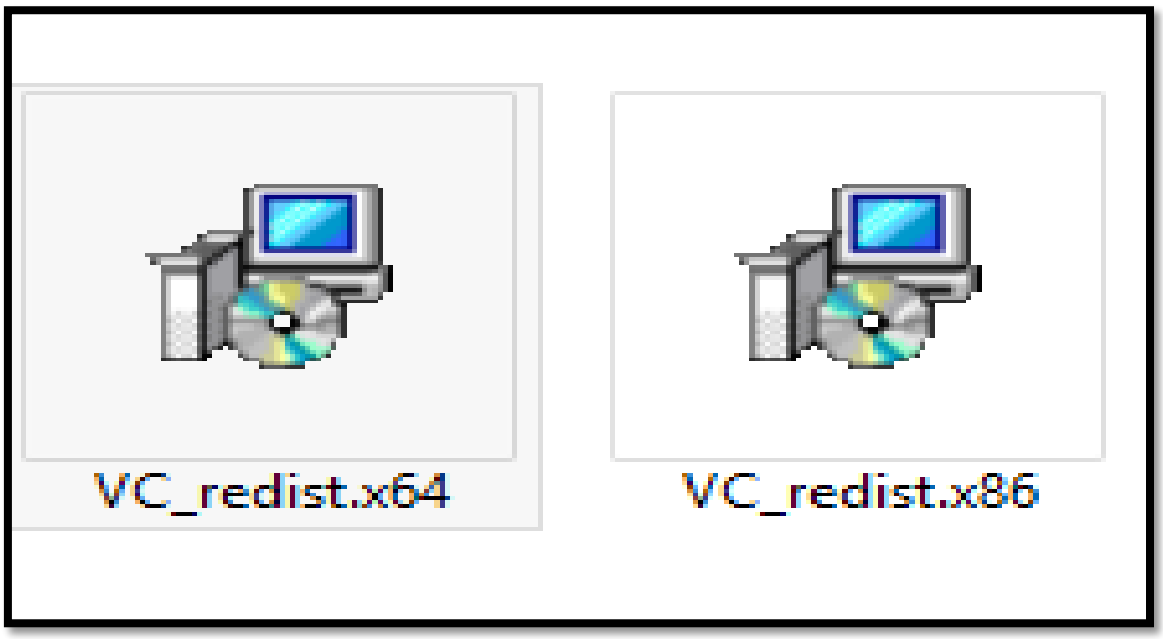
Step 3:- click on latest download



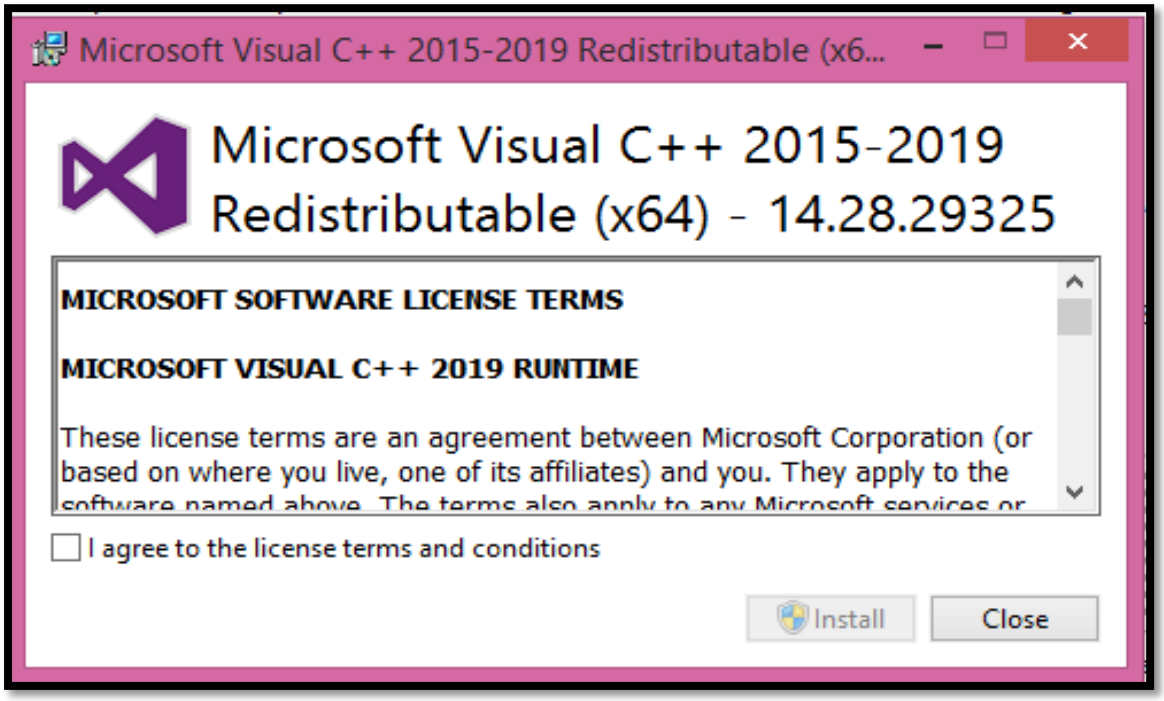
Step 4:- download all support set up



Step5:- Install the Setup

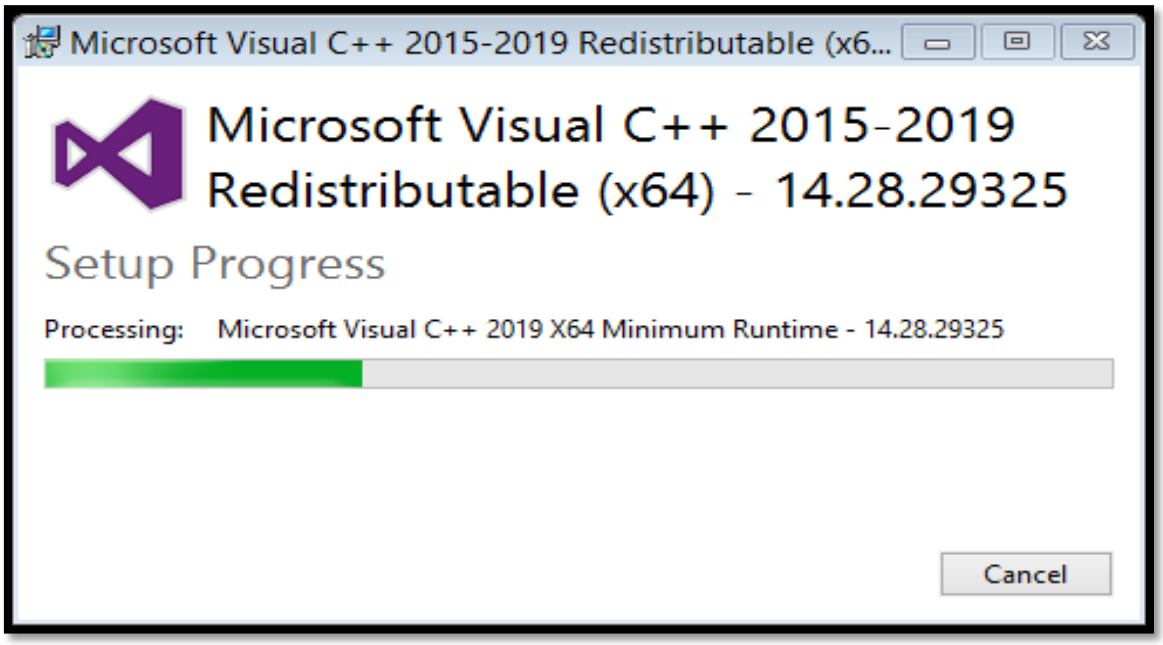


Step: 6:- agreement to policy and condition

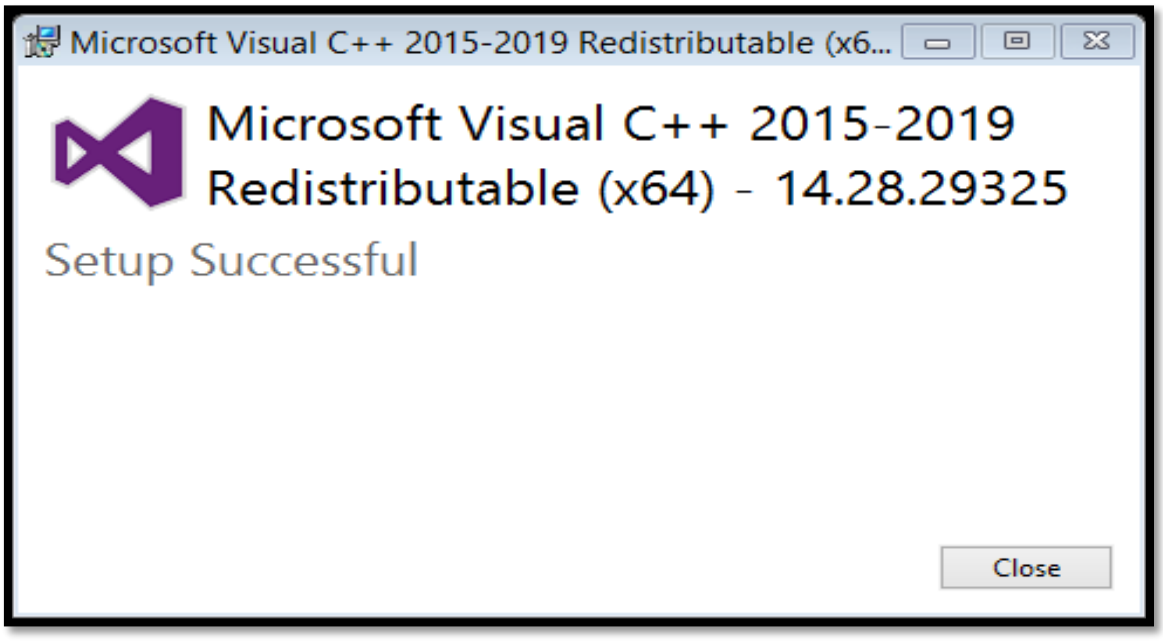


Installation and completion

Step 1:- Install Microsoft Visual



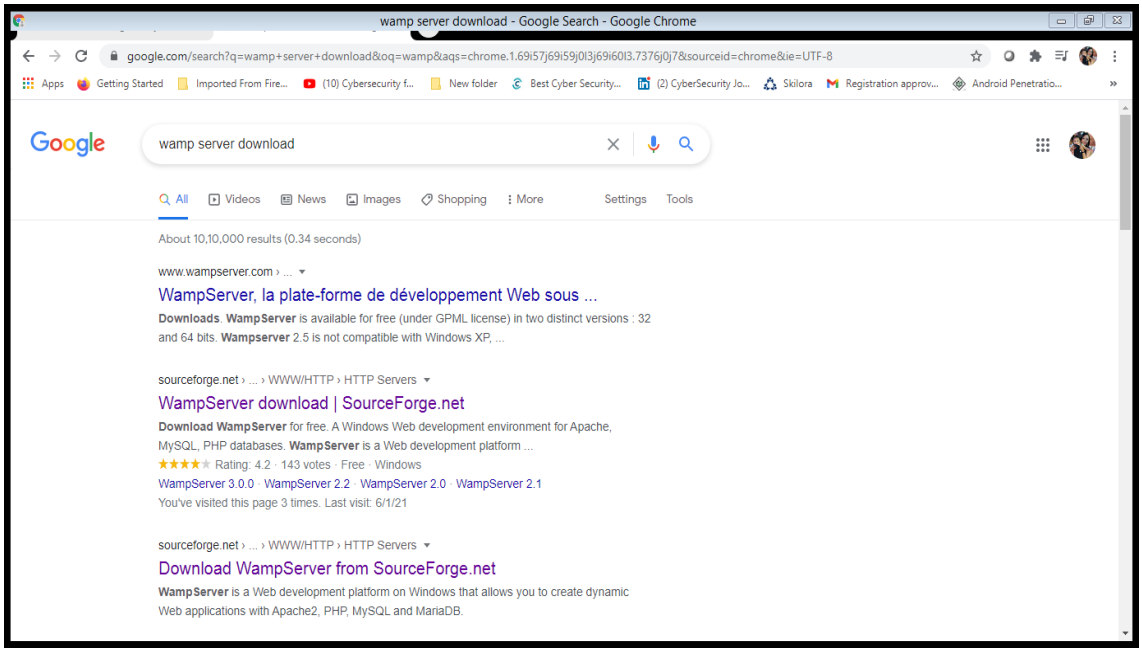
Step 1:- Setup Successful



Introduction to Wamp Server

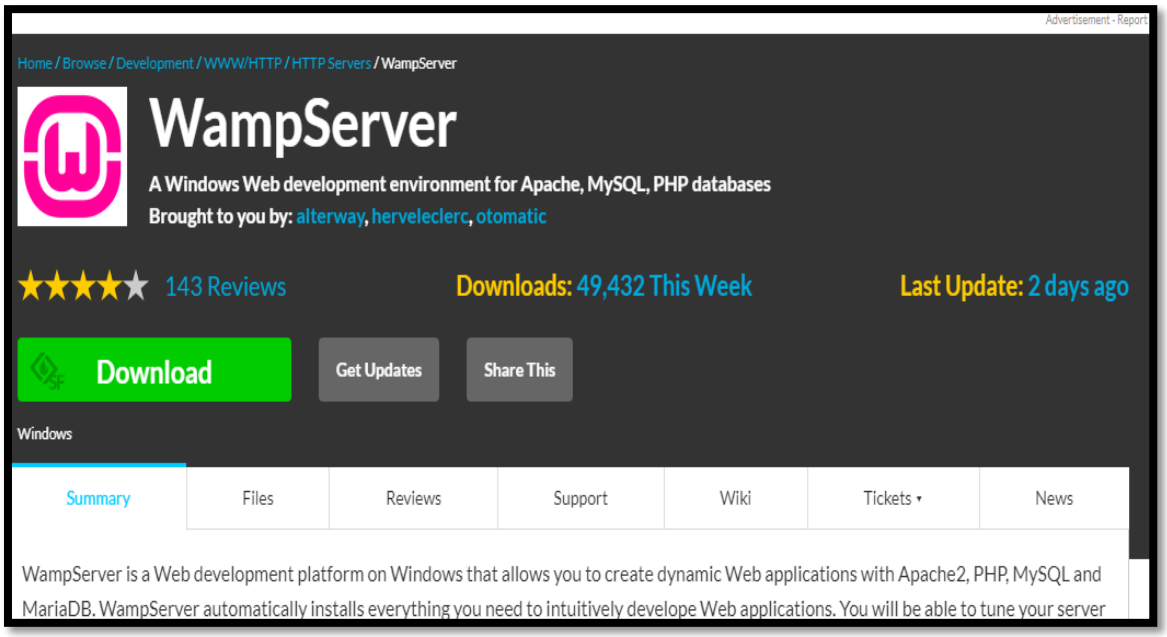
Wamp Server refers to a solution stack for the Microsoft Windows operating system, created by Romain Bourdon and consisting of the Apache web server, Open SSL for SSL support, MySQL database and PHP programming language. Stands for "Windows, Apache, MySQL, and PHP." WAMP is a variation of LAMP for Windows systems and is often installed as a software bundle (Apache, MySQL, and PHP). It is often used for web development and internal testing but may also be used to serve live websites.

Step 1:- Download Wamp Server



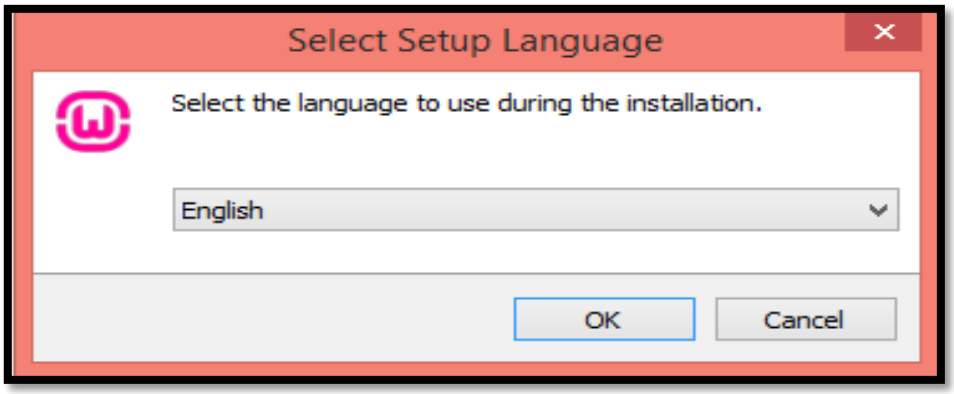
Step 2:- Download Wamp From Given Site

Step 3:- click on download

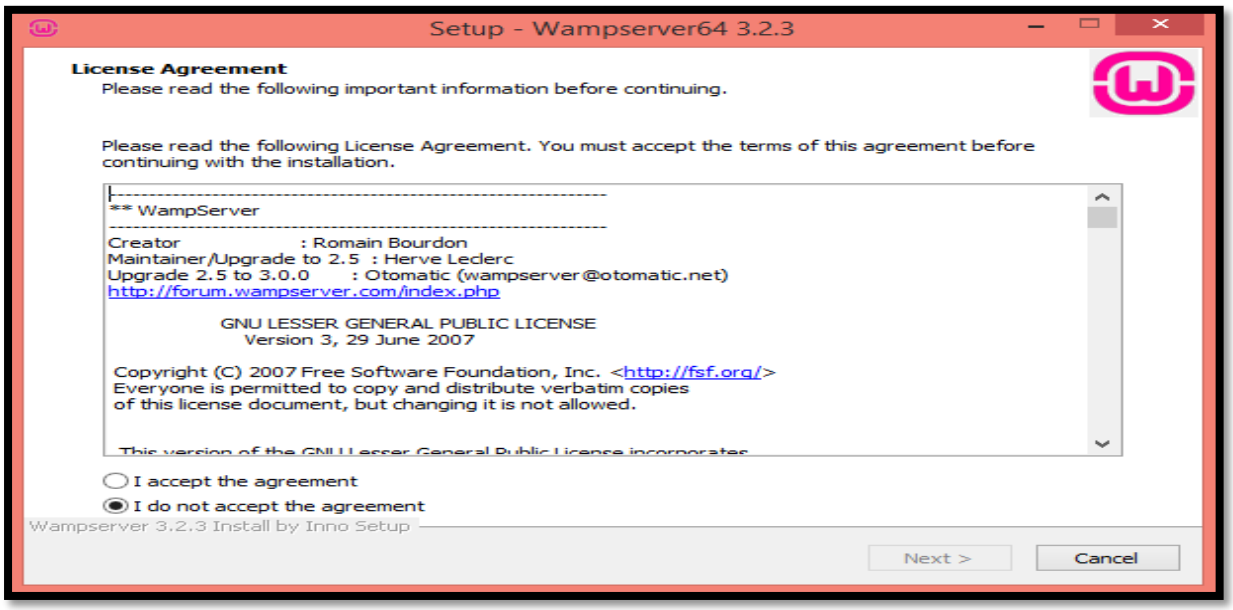


Now it is downloaded in our system

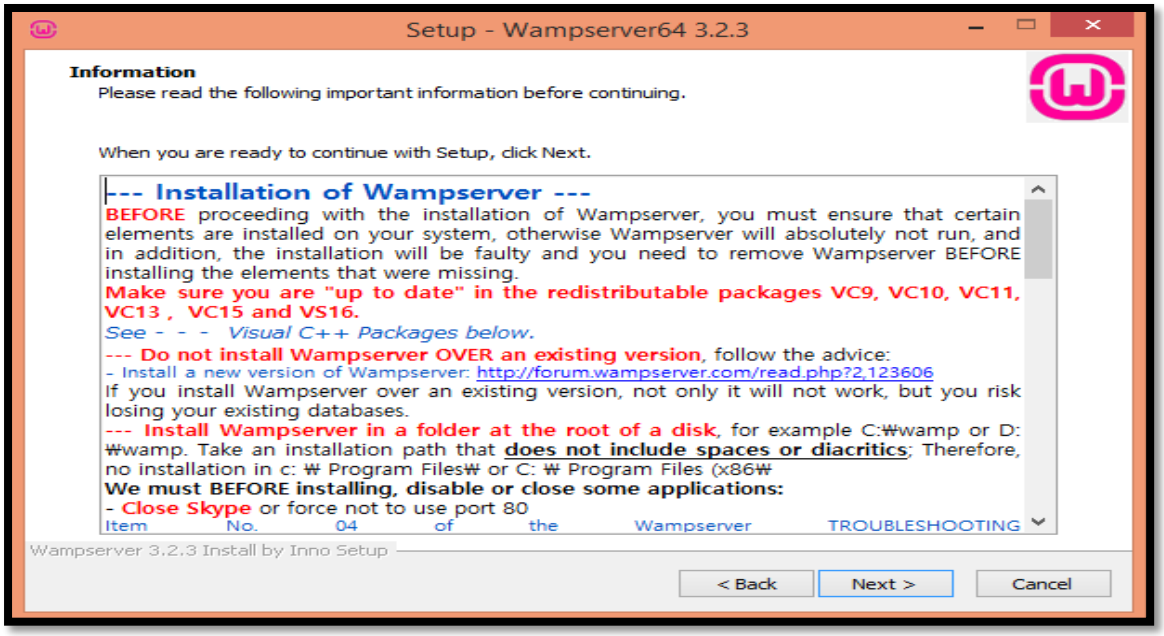
Step 4:- click on language and ok



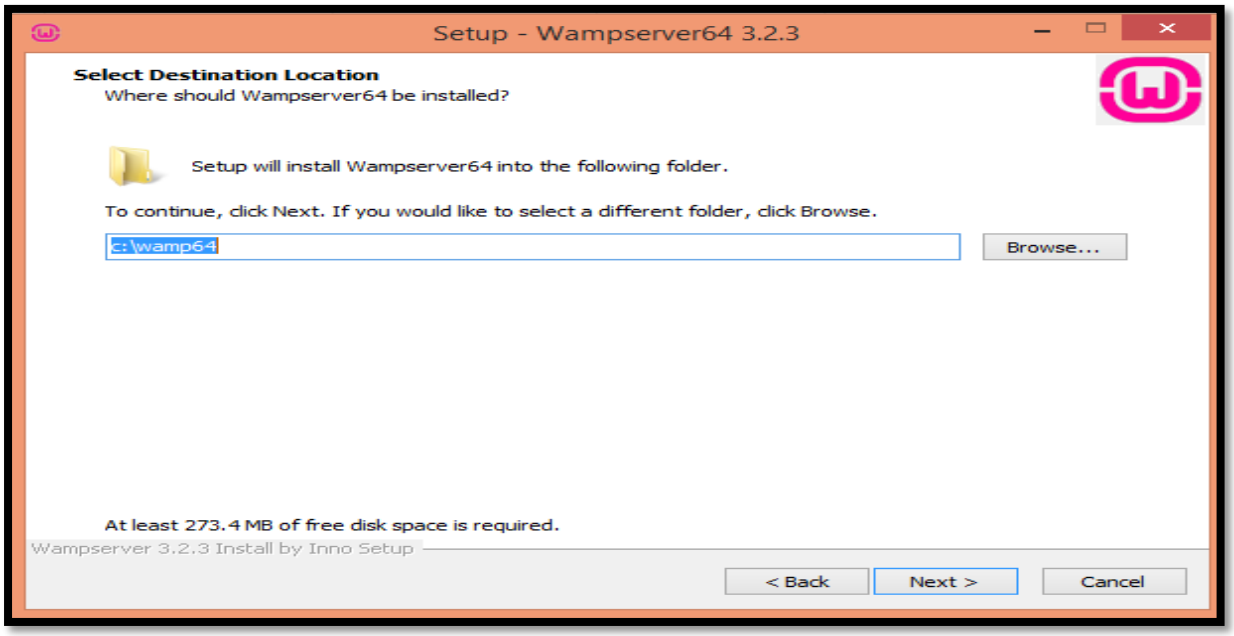
Step 5:- click on I accept



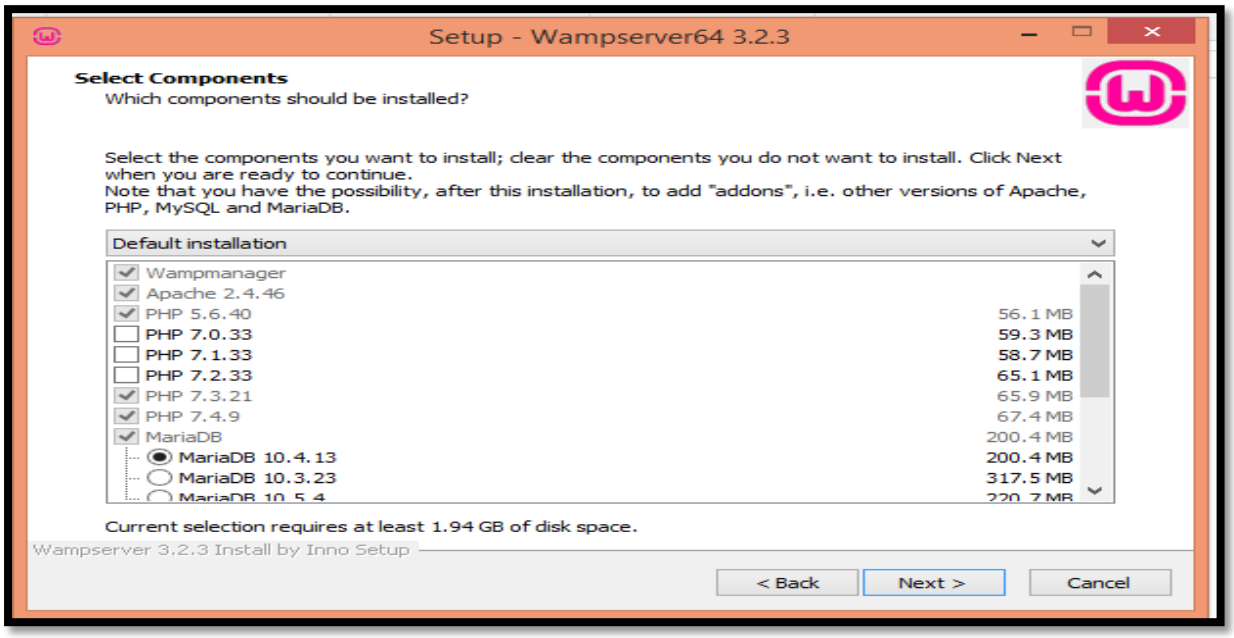
Step 6:- On Information Wizard Click On Next



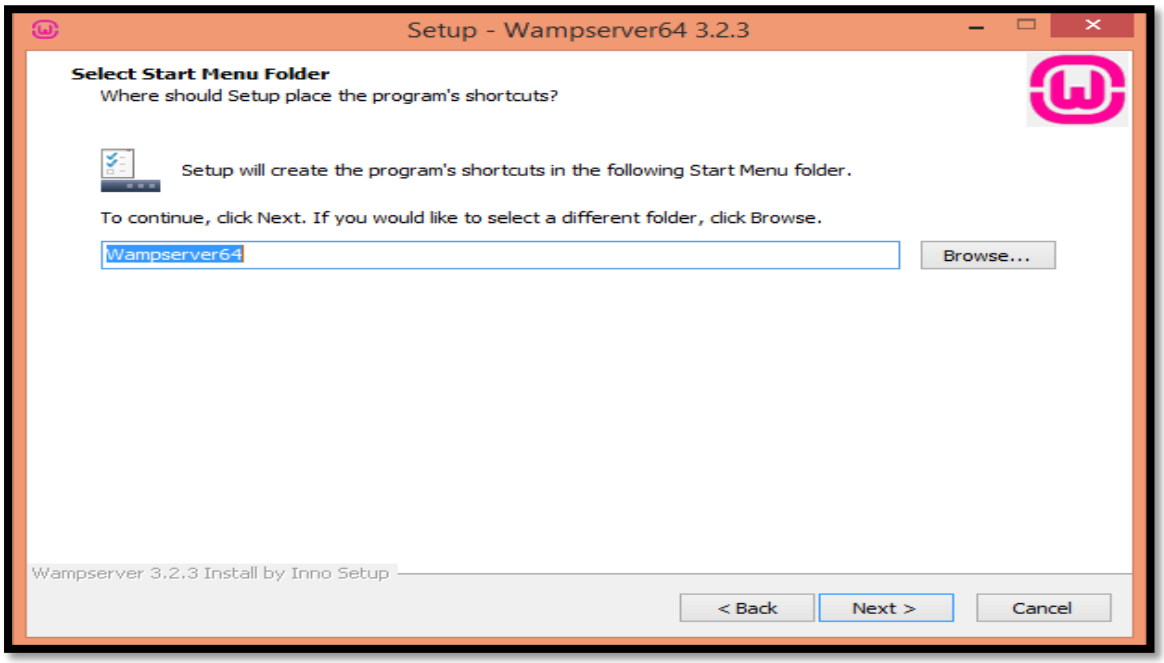
Step 7:- Select the destination click on next



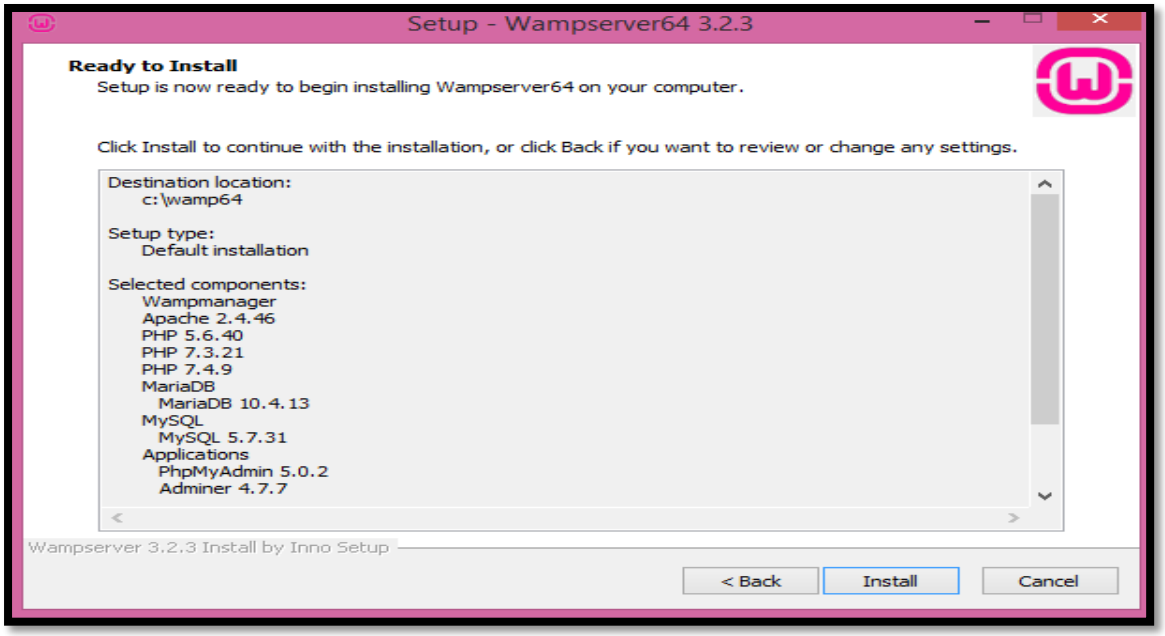
Step 8:- Select components



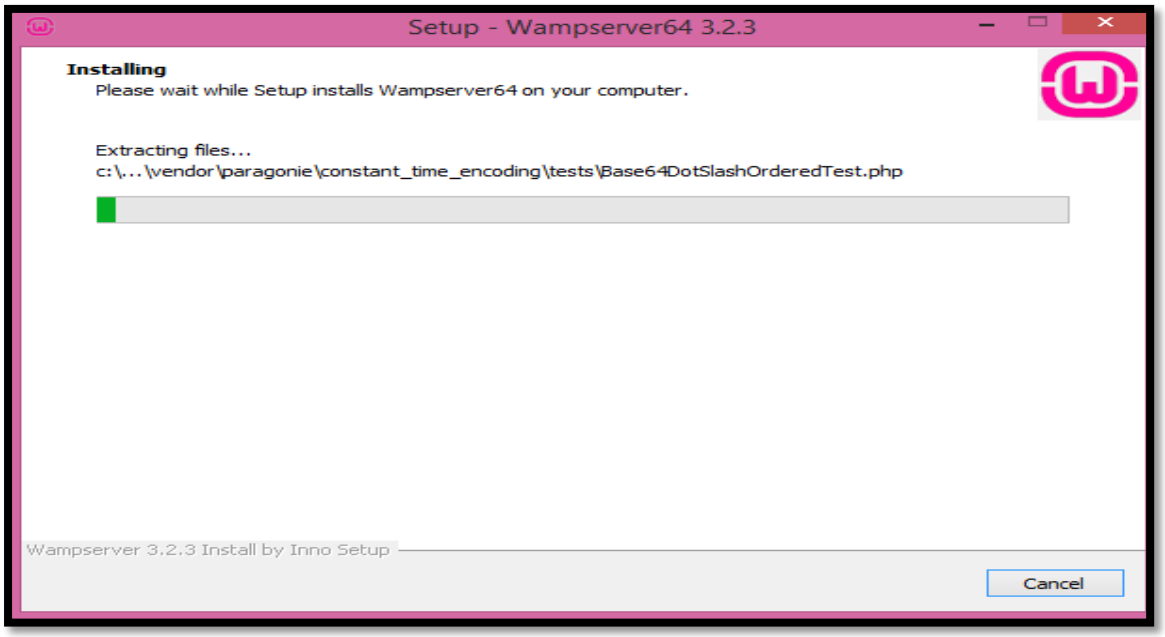
Step 9:- We can edit the name



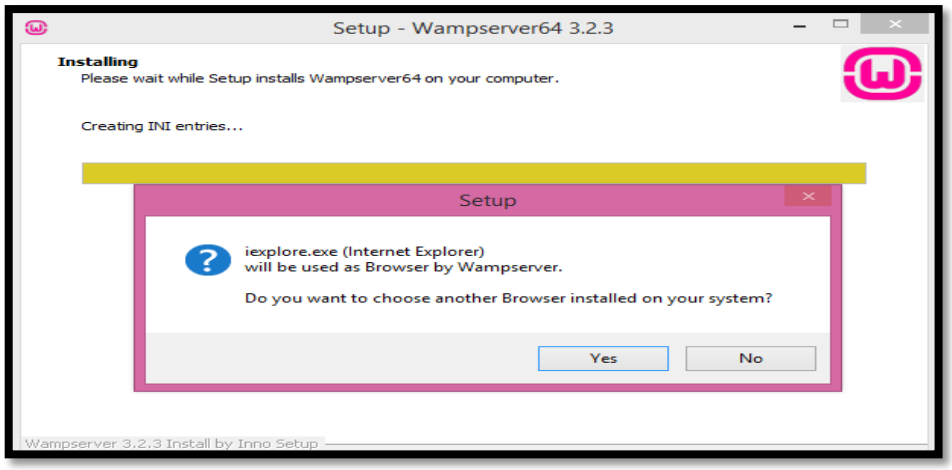
Step 10:- Showing the installation is ready

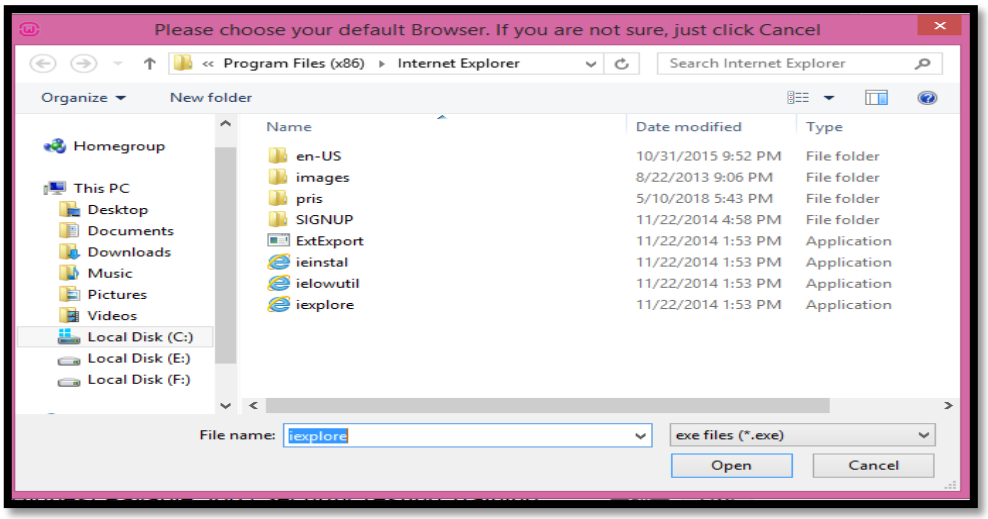


Step 11:- Installation process is going on

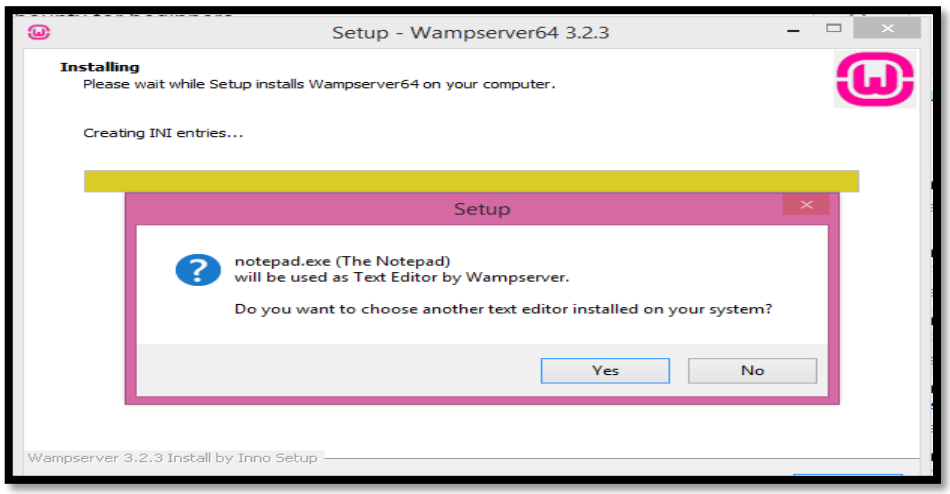


Step 12:-Click on yes for linking to web browser

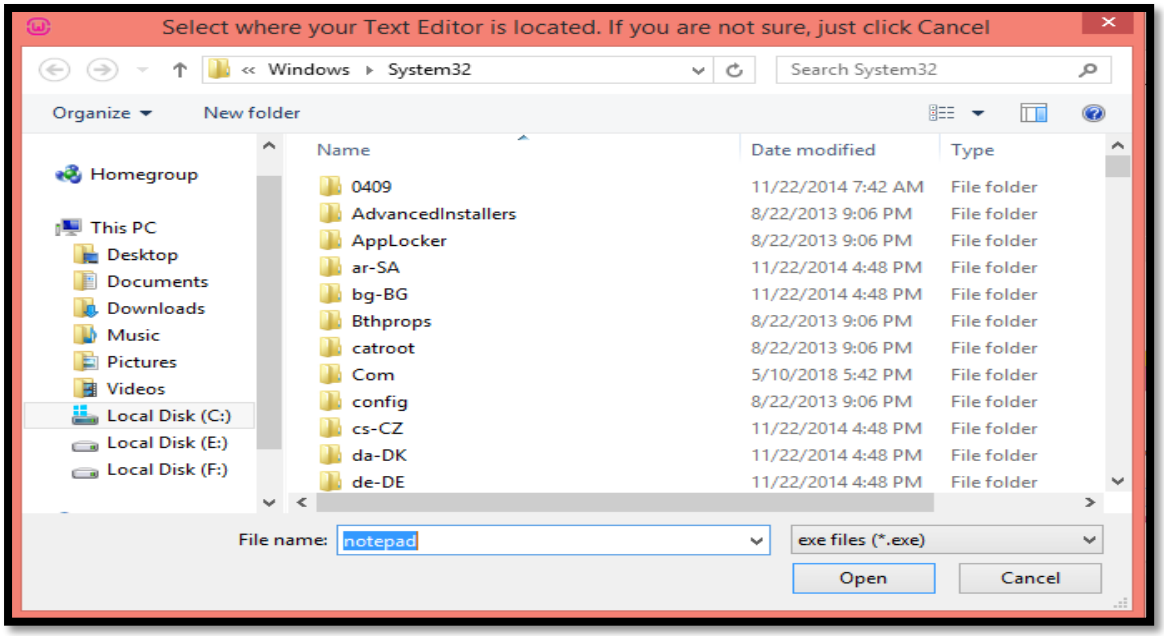




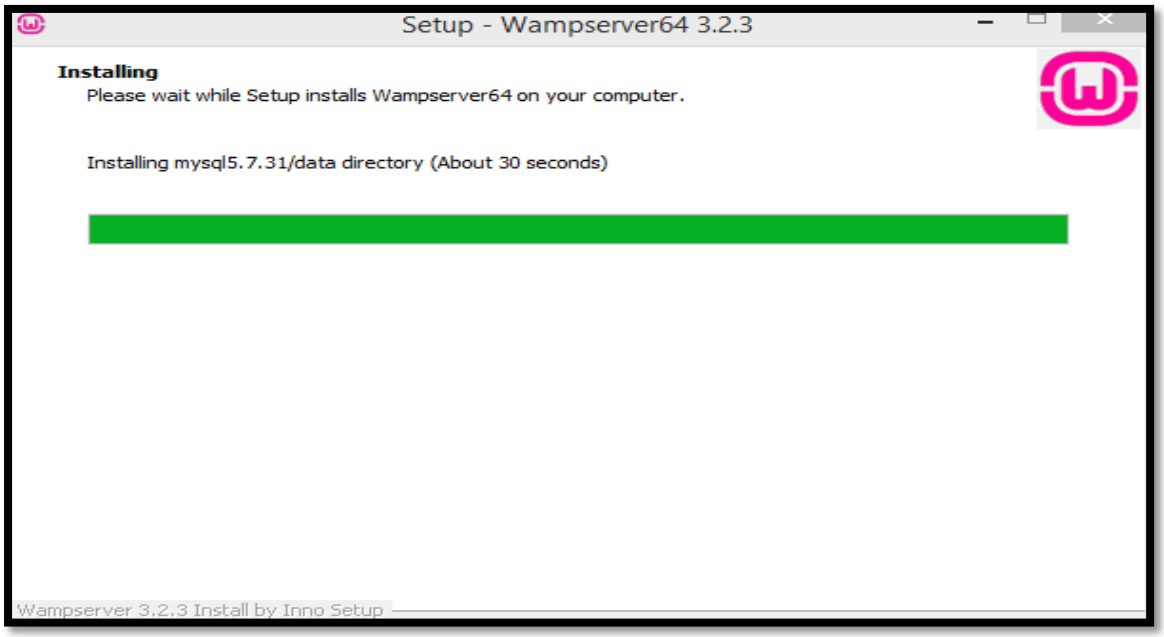
Step13:- Linking notepad

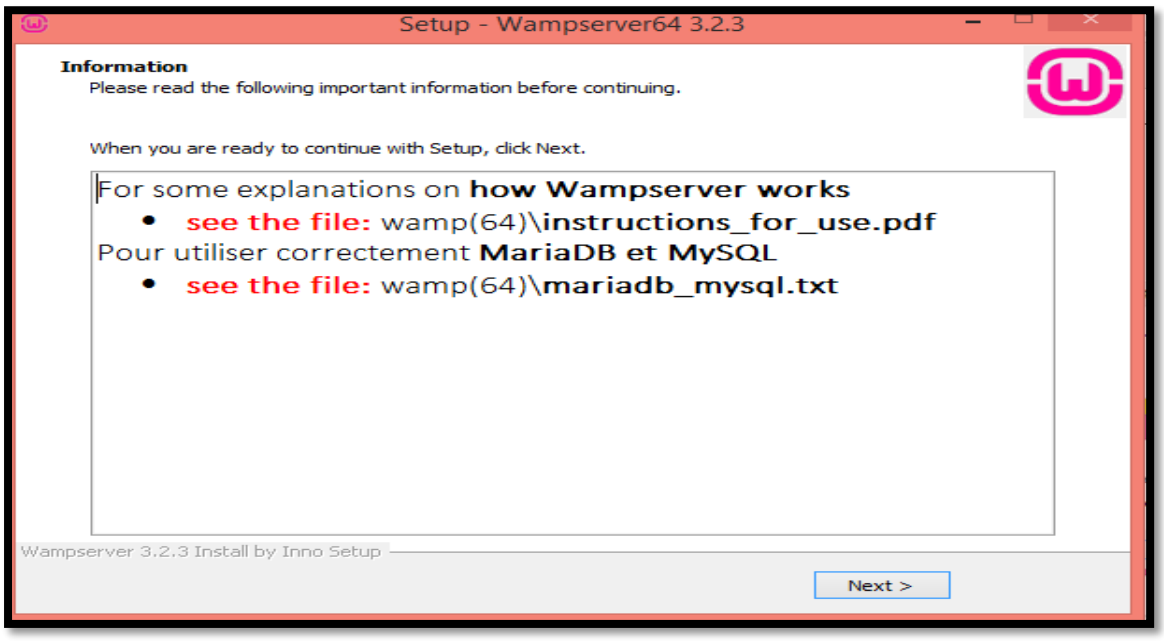


Step 14:- Select destination location



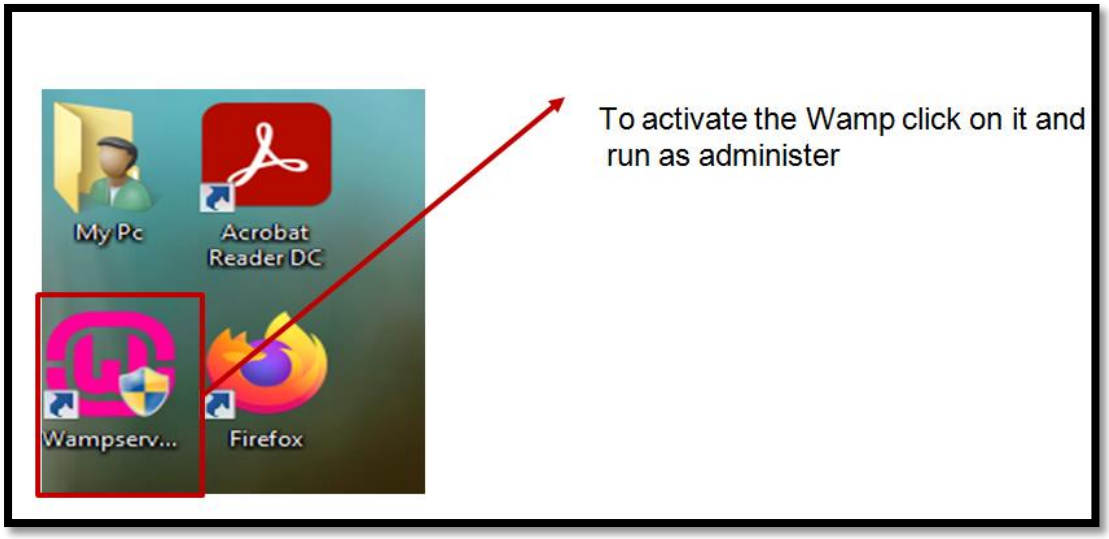
Step 15:- Installation and Warning



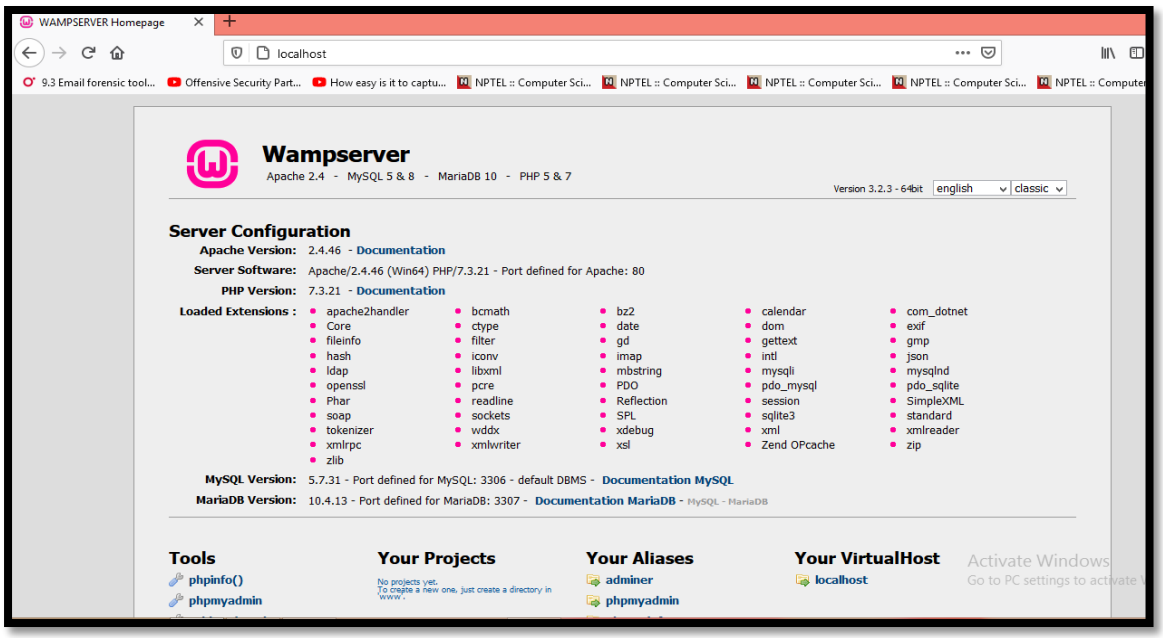


Step 16:- Click on finish

To activate WAMP



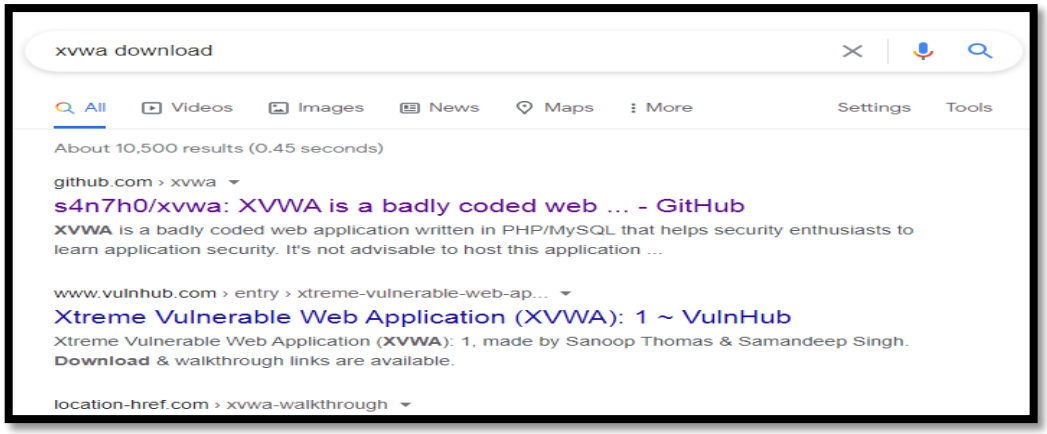
In Firefox write local host



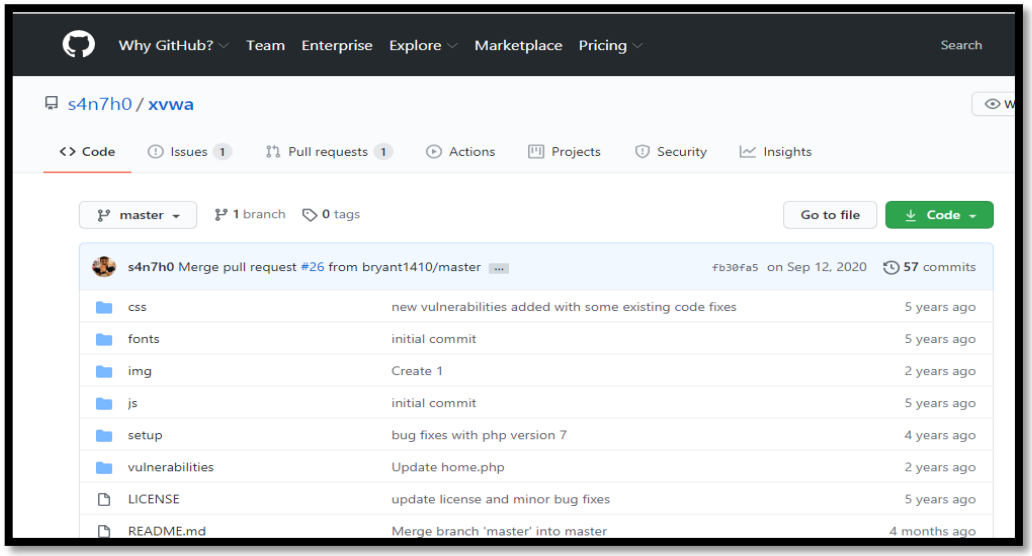
Introduction to Xtreme Vulnerable Web Application

Xtreme Vulnerable Web Application (XVMA) is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security.

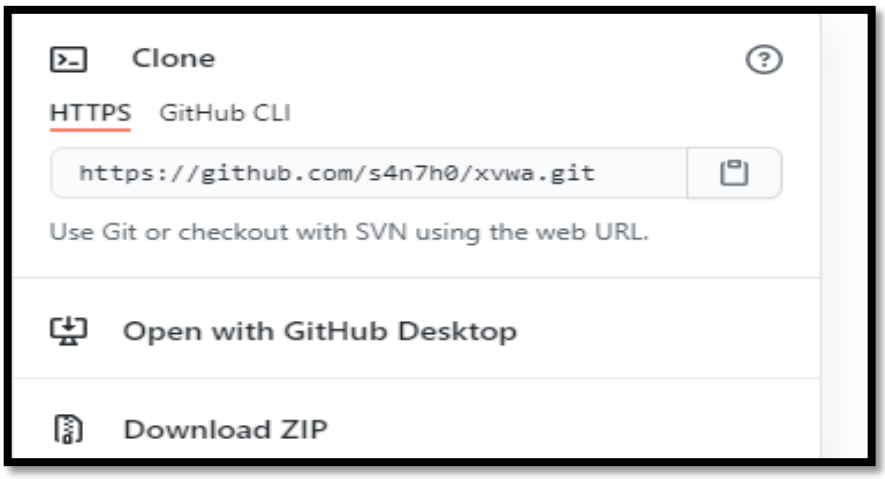
Step1: Type XVWA download in the dialogue box



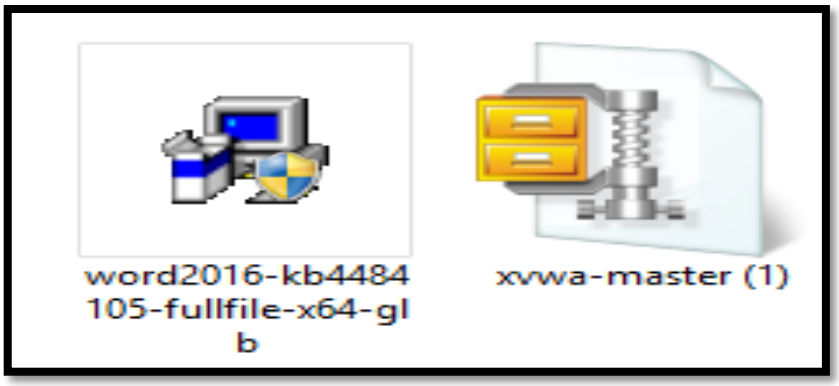
Step 2: After getting XVWA in search



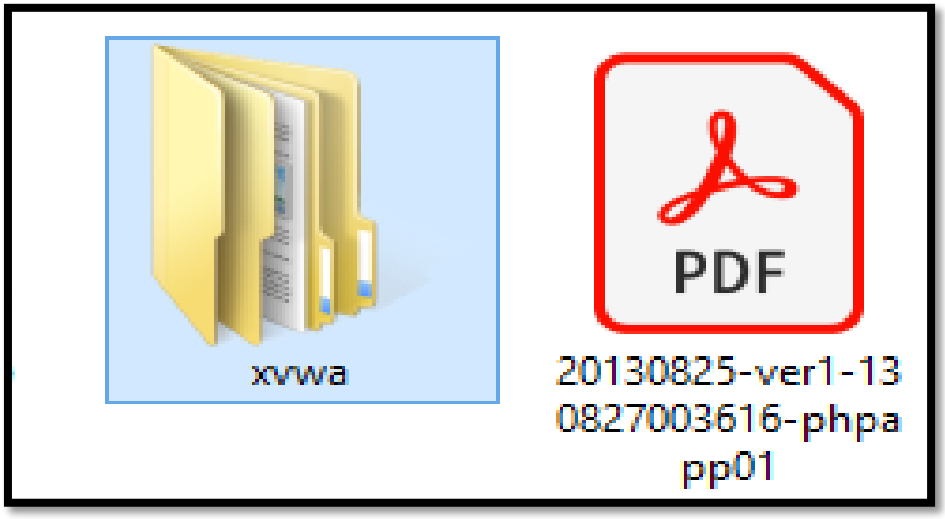
Step 3: Open the website Github



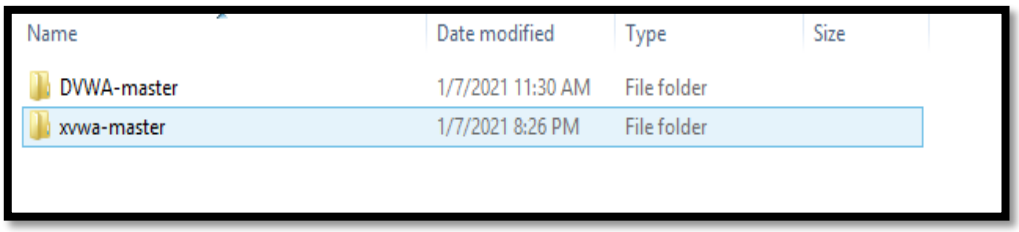
Step 4: Download the ZIP file



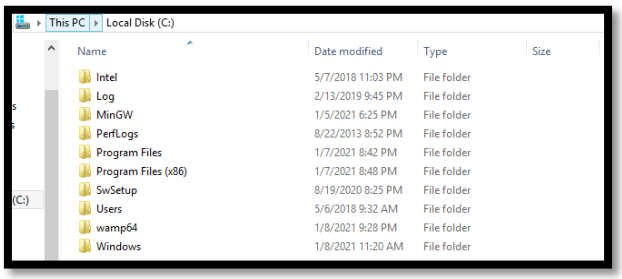
Step 5: Save the folder XVWA



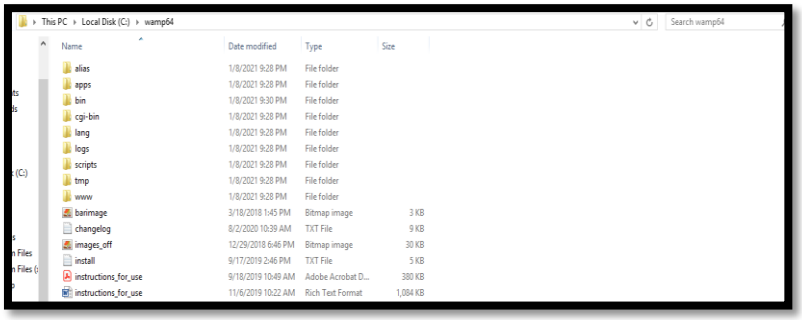
Step 6: Open XVWA-Master folder



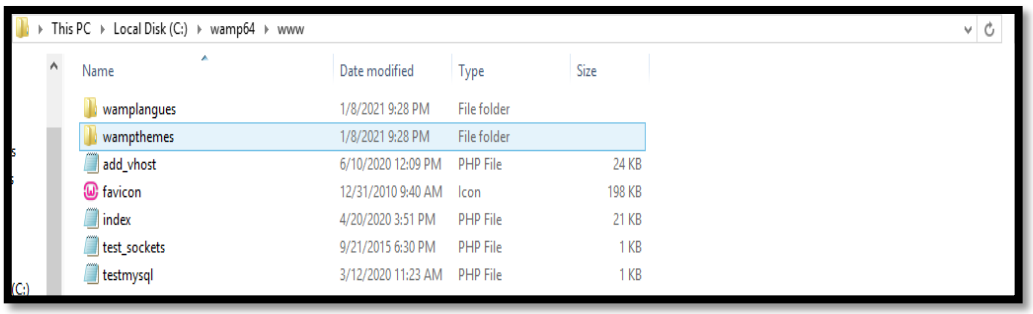
Step 7: Search for wamp64 folder



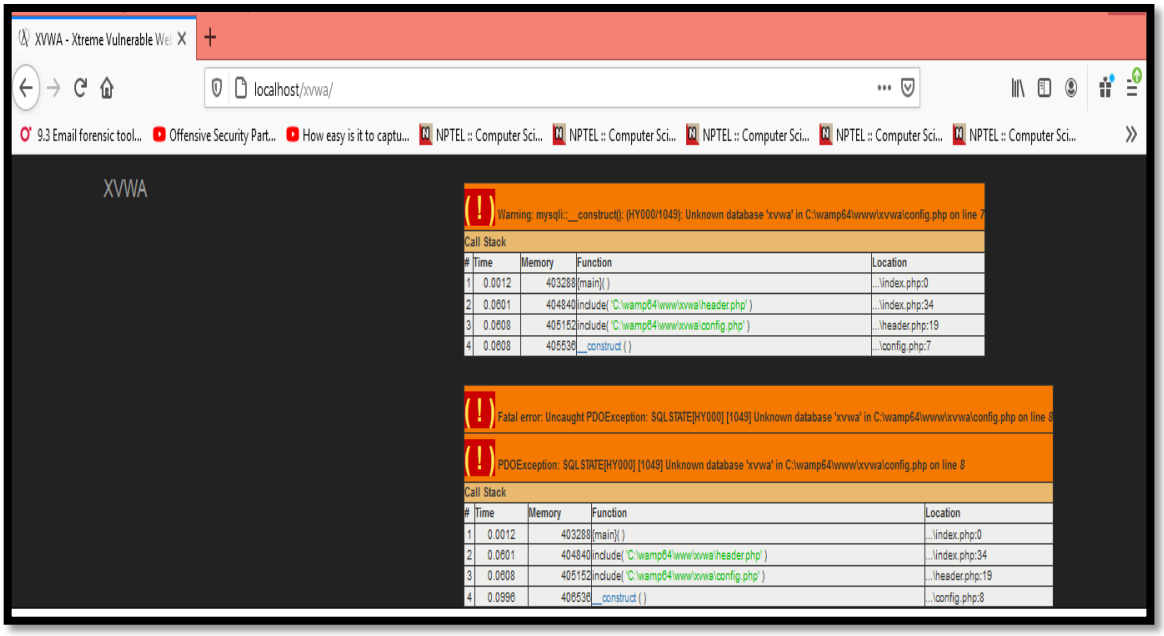
Step 8: Open wamp64 folder



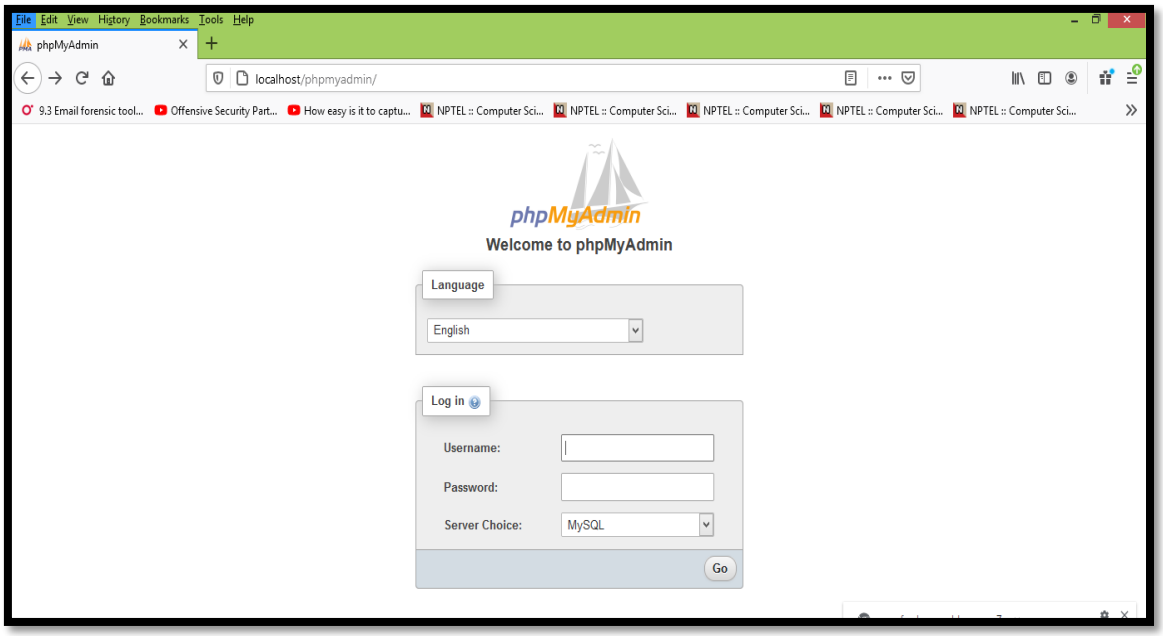
Step 9: Then Open wampthemes folder



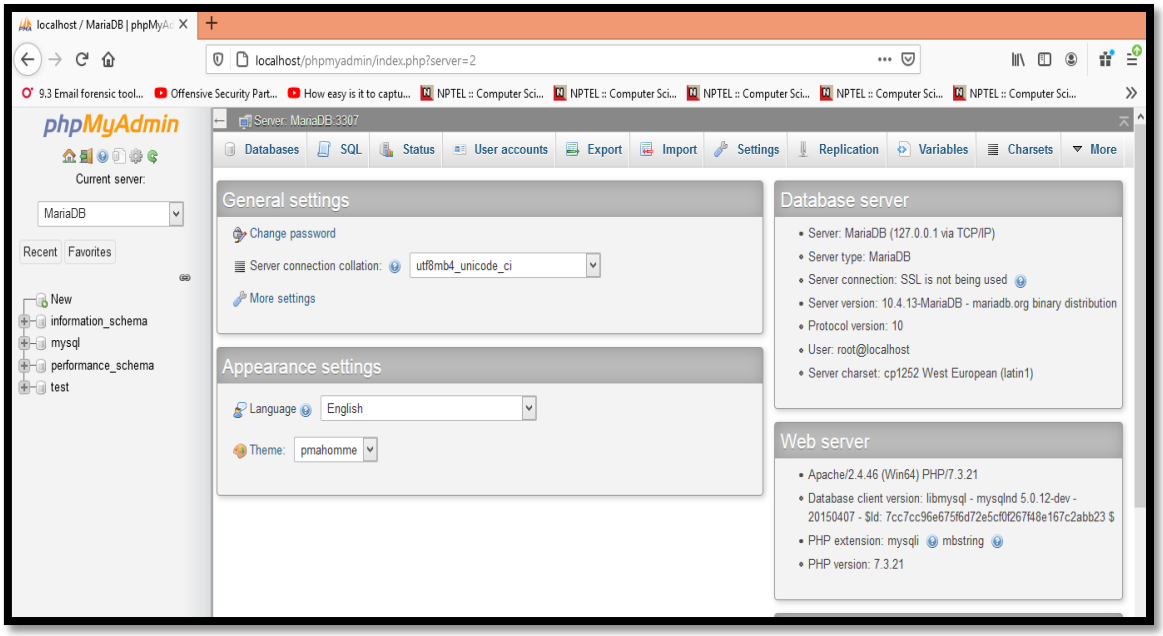
Step 10: Run xvwa in local server



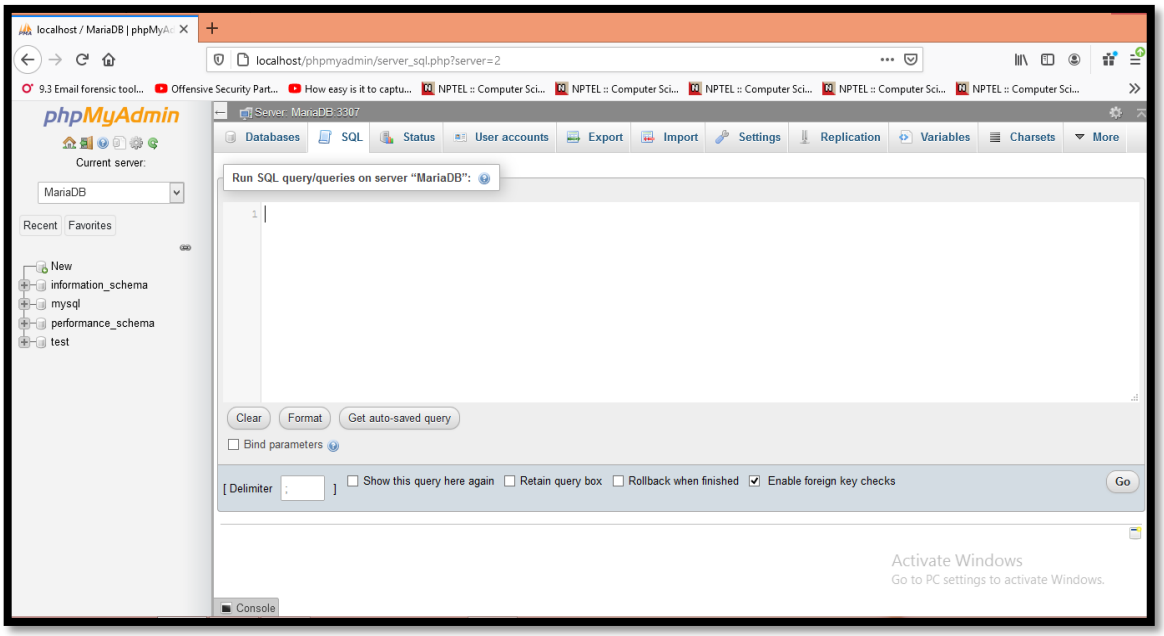
Step 11: Fill login credentials



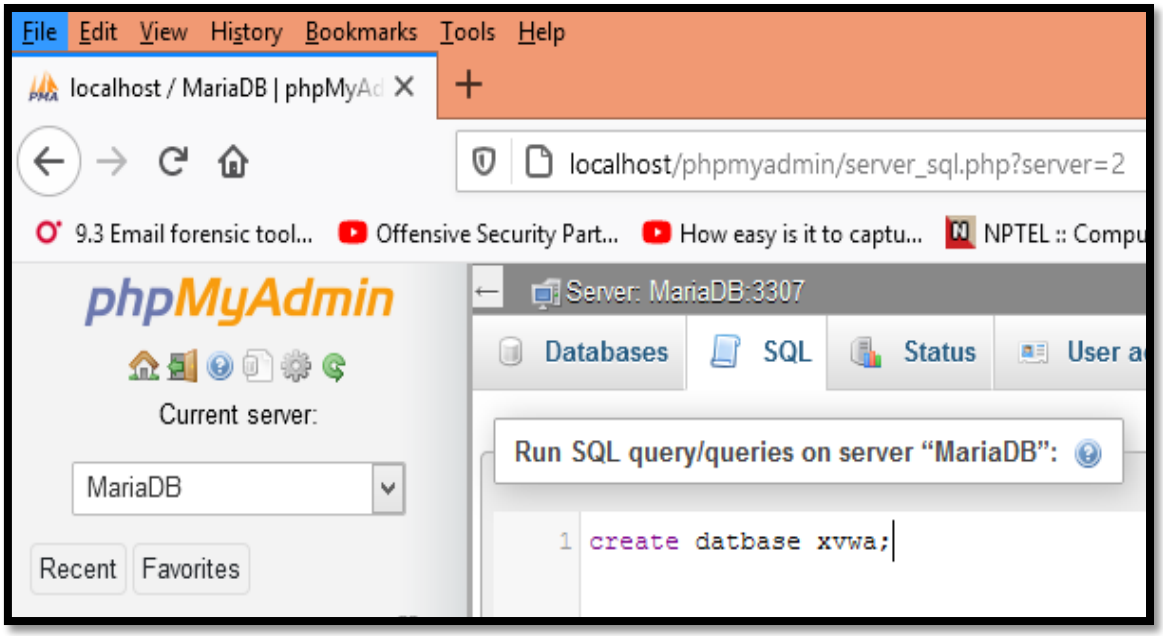
Step 12: Here it is showing the General setting



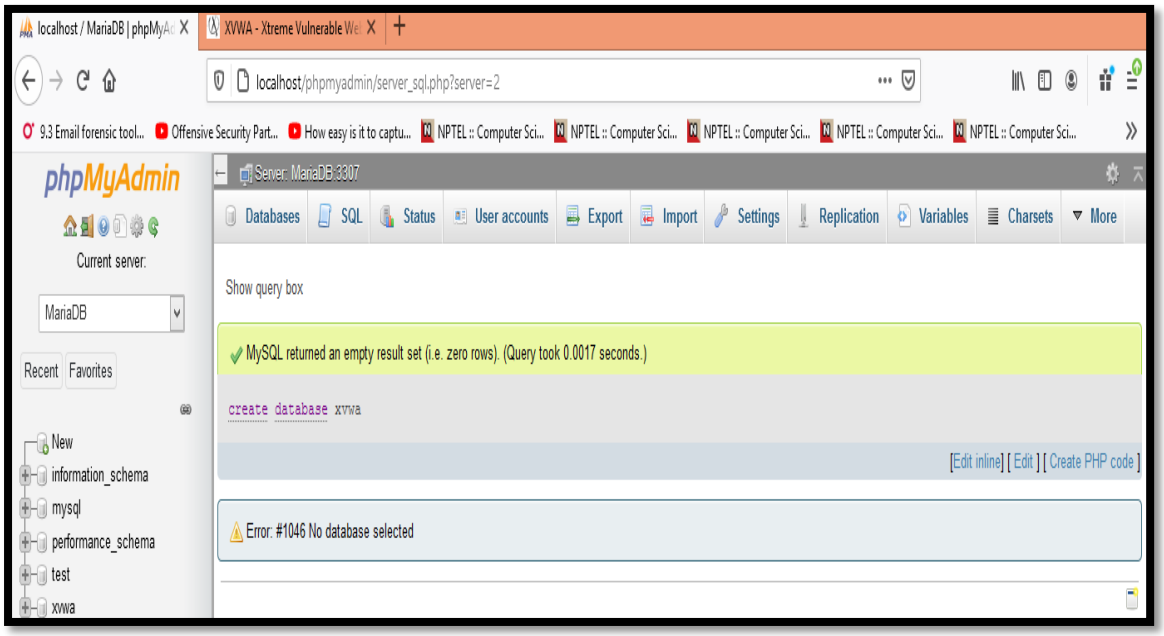
Step 13: Run SQL query/queries



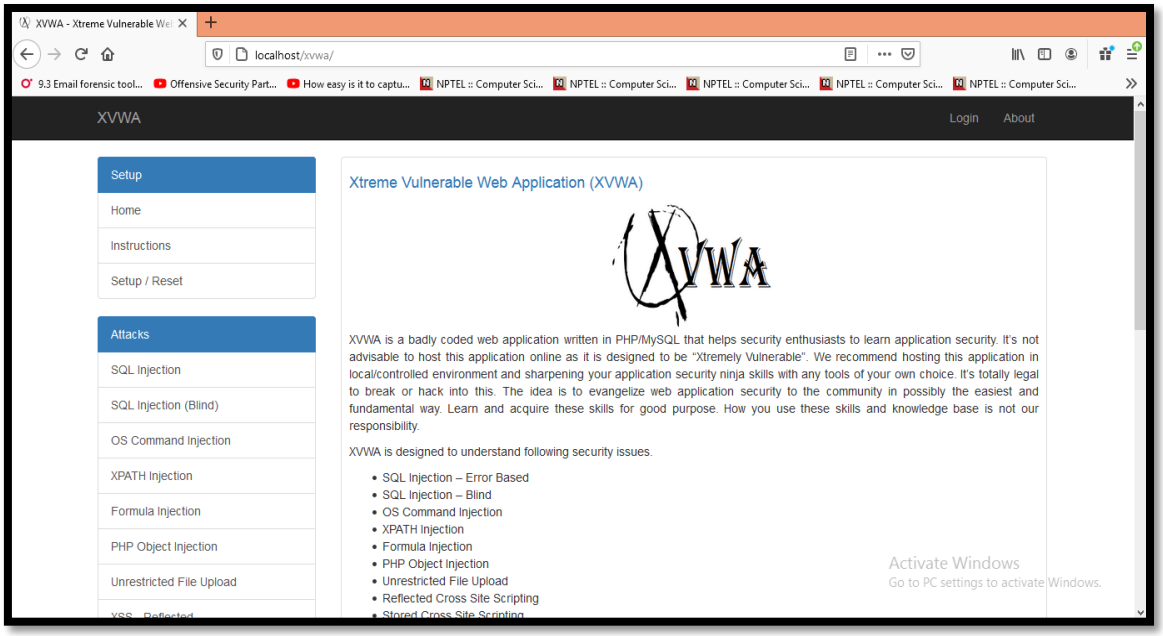
Step 14: Click on SQL > then run query.



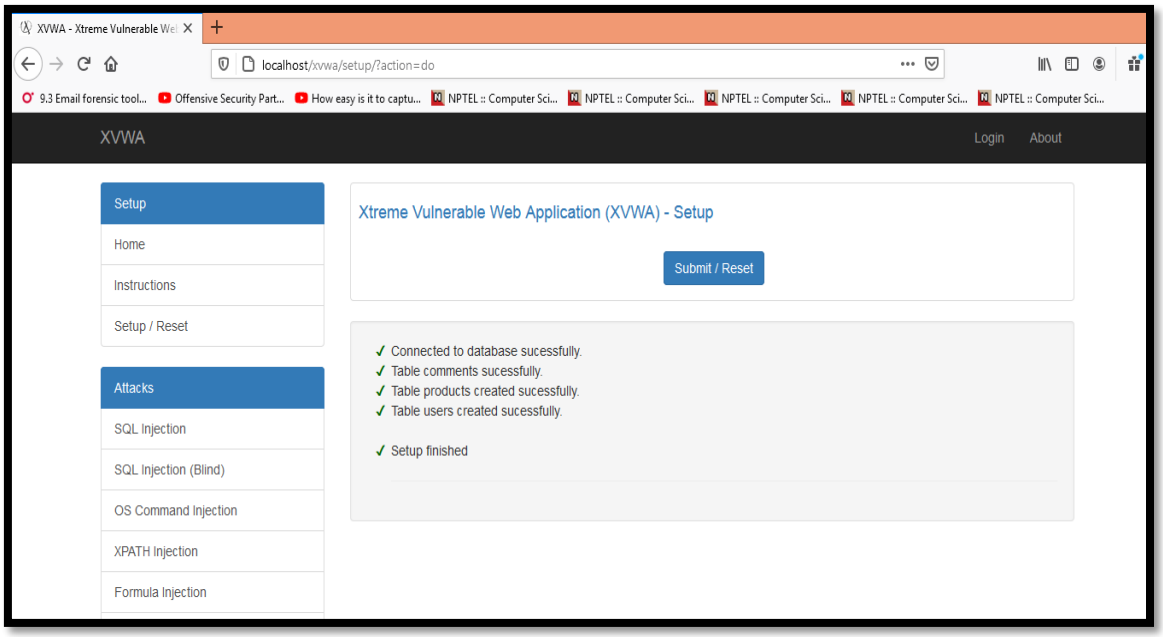
Step 15: MYsql returned an Empty result



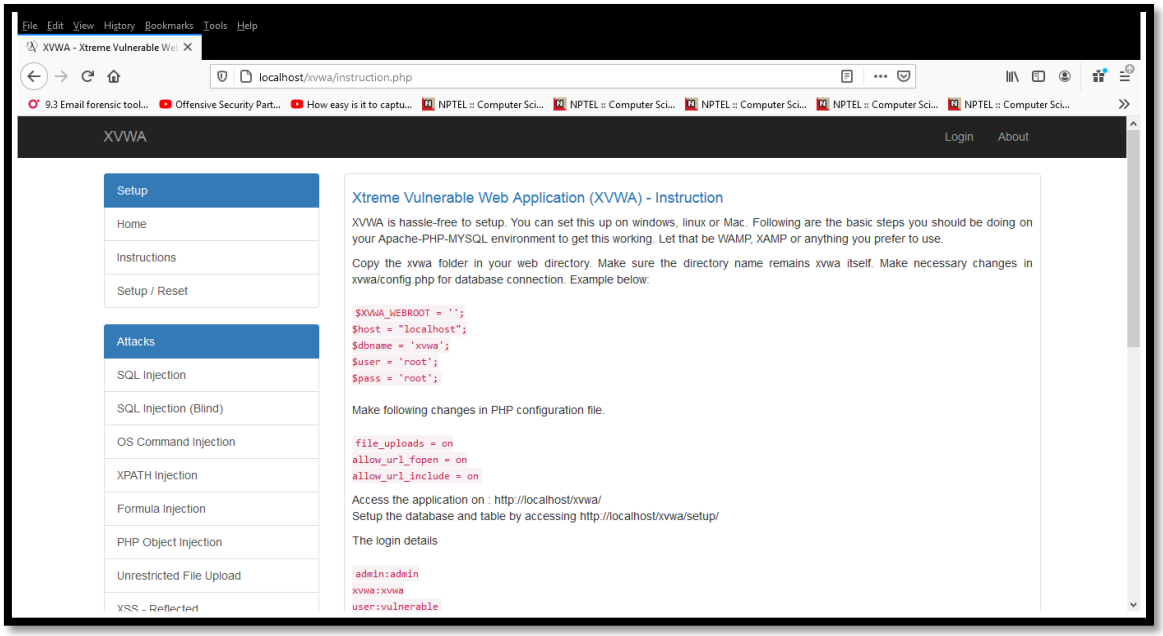
Step 16: Run XVWA in local server



Step 17: Setup Settings



Step 18: XVWA Instruction



Step 19: Fill Credentials to login.